What is claimed is:

CLAIMS

1. A method for content access control operative to enable authorized devices to access protected content and to prevent unauthorized devices from accessing protected content, the method comprising:

providing a plurality of authorized devices;

dividing the plurality of authorized devices into a plurality of groups, each of the plurality of authorized devices being comprised in at least one of the plurality of groups, no two devices of the plurality of authorized devices being comprised in exactly the same groups;

determining whether at least one device of the plurality of authorized devices is to be prevented from having access to the protected content and, if at least one device is to be prevented, removing all groups comprising the at least one device from the plurality of groups, thus producing a set of remaining groups; and

determining an authorized set comprising groups from the set of remaining groups, such that each device of the plurality of authorized devices which was not determined, in the determining whether step, to be prevented from having access is comprised in at least one group of the authorized set.

2. A method according to claim 1 and also comprising:

assigning, to each one of the plurality of authorized devices, a set of keys comprising one group key for each group of which the one device is a member; and

utilizing at least some of the group keys for communication of a content decryption key to at least one of the plurality of authorized devices.

3. A method according to claim 2 and wherein the utilizing step comprises, for each of the plurality of authorized devices:

obtaining the content decryption key, wherein the obtaining comprises performing no more than a predetermined number of decryptions.

4. A method according to claim 2 and wherein the utilizing step comprises, for each of the plurality of authorized devices:

obtaining the content decryption key, wherein the obtaining comprises performing exactly one decryption.

a4

5. A method according to claim 2 and also comprising:

at each authorized device having access to the protected content, performing no more than a predetermined number of decryption operations, said predetermined number being the same for all authorized devices, to obtain the content decryption key from an encrypted form thereof, said encrypted form being encrypted with a group key corresponding to a group of which said authorized device is a member.

05025865.02400

6. A method according to claim 5 and wherein said predetermined number does not depend on the number of authorized devices.

7. A method according to claim 5 and wherein said predetermined number is equal to 1.

8. A method according to claim 2 and also comprising the step of:

at at least one of the authorized devices, using the group key of the set of keys corresponding to the group of which the authorized device is a member.

9. A method according to claim 2 and wherein each group key of the set of keys is assigned an initial value, and said initial value can not be changed.

10. A method according to claim 1 and wherein the authorized set comprises a plurality of maximal groups from the set of remaining groups, such that each maximal group is not a subset of any one of the set of remaining groups.

11. A method according to claim 1 wherein the determining whether step comprises receiving an identification of the at least one device.

12. A method according to claim 1 and wherein each two devices of the plurality of authorized devices have at least one group key in common.

13. A method according to claim 1 and wherein at least some of the authorized devices are not in communication with a central authorization facility after an initial manufacturing period.

14. A method for preventing a plurality of devices, chosen from among a plurality of authorized devices, from having access to protected content, the method comprising:

distributing a protected content access key independently encrypted with each group key of a set of group keys, wherein none of a plurality of devices to be prevented from having access to protected content are members of any group associated with any of the set of group keys.

15. A method according to claim 14 and wherein each group key of the set of group keys has an initial value, and the initial value can not be changed.

16. A method according to claim 14 and also comprising:

at each authorized device having access to the protected content, performing no more than a predetermined number of decryption operations, said predetermined number being the same for all authorized devices, to obtain the protected content access key from an encrypted form thereof, said encrypted form being encrypted with a group key corresponding to a group of which said authorized device is a member.

17. A method according to claim 16 and wherein said predetermined number does not depend on the number of authorized devices.

18. A method according to claim 17 and wherein said predetermined number is equal to 1.

19. A method according to claim 2 and also comprising:

generating each of said group keys as a plurality of independently generated sets of group keys, wherein no group key of any one independently generated set is based, even in part, on any key of any other independently generated set.

20. A method according to claim 14 and also comprising:

generating each of said group keys as a plurality of independently generated sets of group keys, wherein no group key of any one independently generated set is based, even in part, on any key of any other independently generated set.

21. A method according to claim 2 and also comprising:

generating each of said group keys as a plurality of independently generated sets of group keys, wherein each group key is based, at least in part, pseudo-randomly on a source key.

22. A method according to claim 14 and also comprising:

generating each of said group keys as a plurality of independently generated sets of group keys, wherein each group key is based, at least in part, pseudo-randomly on a source key.

23. A method according to claim 2 and also comprising:

dividing the plurality of groups into a hierarchical set of groups, said hierarchical set of groups comprising a plurality of groups comprising at least a first group and a second group, each of said first group and said second group being associated with first and second group key generation information respectively; and

generating a least one group key in each of said first group and said second group using said associated group key generation information, wherein

said second group key generation information can be derived from said first group key generation information.

24. A method according to claim 14 and also comprising:

dividing the plurality of groups into a hierarchical set of groups, said hierarchical set of groups comprising a plurality of groups comprising at least a first group and a second group, each of said first group and said second group being associated with first and second group key generation information respectively; and

generating a least one group key in each of said first group and said second group using said associated group key generation information, wherein

said second group key generation information can be derived from said first group key generation information.

25. A method according to claim 23 and wherein said second group is a subgroup of said first group.

26. A method according to claim 23 and wherein said first group key generation information can not be derived from said second group key generation information.

27. A method according to claim 23 and wherein at least one of said first group key generation information and said second group key generation information is embedded in at least one removable security device.

28. A method according to claim 27 and wherein said at least one removable security device comprises, for at least one of said first group and said second group, a plurality of removable security devices.

29. A method according to claim 28 and wherein at least a predetermined portion of said plurality of removable security devices is required for determining the associated group key generation information.

30. A security element comprising:

a secret store operative to store a secret s;

a first output path for outputting s; and

a second output path for outputting f(s), where f is a function,

wherein said first output path is functional only during a first period.

31. Apparatus according to claim 30 and wherein f=g(x), where x is an input value.

32. Apparatus according to claim 30 and wherein the first period continues until the first output path has been used a predetermined number of times.

33. Apparatus according to claim 30 and wherein the first output path is functional for a predefined period of time.

34. Apparatus according to claim 30 and wherein the first output path is functional until a first predefined command is received by the security element.

35. Apparatus according to claim 30 and wherein the first period begins upon receipt of a second predefined command by the security element.

36. Apparatus according to claim 34 and also comprising an external communication module, and

wherein at least one of the following is received from a source external to the security element, via the external communication module: the first predefined command; and the second predefined command.

37. Apparatus according to claim 30 and wherein the security element also comprises:

a secret derivation unit operative to derive the secret s from a supplied input.

38. Apparatus according to claim 37 and wherein the secret derivation unit is operative to derive the secret s from the supplied input based, at least in part, on pseudo-random generation.

39. Apparatus according to claim 37 and wherein the supplied input is supplied by a key escrow unit external to the security element.

40. Apparatus according to claim 30 and wherein the secret s is supplied by a key escrow unit external to the security element.

41. Apparatus according to claim 30 and wherein the security element functions as a key escrow component.

42. A system for content access control operative to enable authorized devices to access protected content and to prevent unauthorized devices from accessing protected content, the system comprising:

grouping apparatus operative to divide a plurality of authorized devices into a plurality of groups, each of the plurality of authorized devices being comprised in at least one of the plurality of groups, no two devices of the plurality of authorized devices being comprised in exactly the same groups;

prevention determination apparatus operative to determine whether at least one device of the plurality of authorized devices is to be prevented from having access to the protected content and, if at least one device is to be prevented, to remove all groups comprising the at least one device from the plurality of groups, thus producing a set of remaining groups; and

authorized set determination apparatus operative to determine an authorized set comprising groups from the set of remaining groups, such that each

device of the plurality of authorized devices which was not determined, in the determining whether step, to be prevented from having access is comprised in at least one group of the authorized set.

43. A system according to claim 42 and also comprising:

key assignment apparatus operative to assign, to each one of the plurality of authorized devices, a set of keys comprising one group key for each group of which the one device is a member; and

utilization apparatus operative to utilize at least some of the group keys for communication of a content decryption key to at least one of the plurality of authorized devices.

44. A method for black box analysis of a device capable of accessing protected content, the method comprising:

providing a device to be analyzed;

inputting to the device a data item comprising encrypted protected content and a plurality of encrypted versions of a content key for accessing the protected content, each of the plurality of encrypted versions being encrypted in accordance with a different one of a plurality of group keys;

receiving, from the device, decrypted content representing a decryption of the protected content;

determining whether the received content is one of the following: erroneous; and null, and producing a result;

identifying a set of group keys comprising at least one group key which is known to the device based, at least in part, on the result,

wherein the data item also comprises at least one invalid content key encrypted in accordance with one of the plurality of group keys.

45. A method for black box analysis of a device capable of accessing protected content, the method comprising:

providing a device to be analyzed;

inputting to the device a data item comprising encrypted protected content and a plurality of encrypted versions of a content key for accessing the protected content, each of the plurality of encrypted versions being encrypted in accordance with a different one of a plurality of group keys;

receiving, from the device, decrypted content representing a decryption of the protected content;

determining whether the received content is one of the following: erroneous; and null and producing a result;

identifying a set of group keys comprising at least one group key which is known to the device based, at least in part, on the result,

wherein the data item also comprises at least one invalid content key encrypted in accordance with one of the plurality of group keys, and

the protected content is protected in accordance with the method of claim 1.

46. A method according to claim 44 and also comprising performing the following steps at least once before performing the identifying step:

choosing a new plurality of encrypted versions of the content key; and

performing the inputting, receiving and determining steps.

47. A method according to claim 46 and wherein the choosing a new plurality step comprises choosing based, at least in part, on at least one of the following:

at least one result of the determining step performed before the choosing step; and

the plurality of encrypted versions of the content key used in the inputting step performed before the choosing step.

48. A method according to claim 44 and wherein the identifying step comprises identifying the one of the plurality of group keys with which the invalid content key is encrypted.

49. A method according to claim 44 and wherein the identifying step comprises identifying a group key which is not one of the plurality of group keys with which the invalid content key is encrypted.

50. A method according to claim 44 and wherein the identifying step comprises identifying a group key which is one of the plurality of group keys with which the invalid content key is encrypted.

05025869.021400